



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Am

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/815,560	03/23/2001	Ari Juels	RSA-045	7481

23483 7590 05/20/2005

WILMER CUTLER PICKERING HALE AND DORR LLP
60 STATE STREET
BOSTON, MA 02109

EXAMINER

JUNG, DAVID YIUK

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 05/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/815,560

Applicant(s)

JUELS ET AL.

Examiner

David Y. Jung

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 March 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-71 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-71 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

CLAIMS PRESENTED

Claims 1-71 are presented.

PRIOR ART

The art made of record and not relied upon is considered pertinent to applicant's disclosure. The art disclosed general background. In particular, note the steganography in <http://www.cotse.com/tools/stega.htm>.

Response to Arguments

Applicant's arguments filed have been fully considered but they are not persuasive. The crux of Applicant's argument appears to regard the error-correcting codes. Yet, the Examiner is unaware of any situation similar to the claimed invention in which the error-correcting code is NOT suggested. Unless the Applicant is willing to dispute this issue, the arguments are not convincing.

CLAIM REJECTIONS

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

Patentability shall not be negated by the manner in which the invention was made.

Claims 1-71 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cottrell (US Patent 5,465,084).

Regarding claim 1, Cottrell teaches "A method for establishing a secret to authenticate a user comprising the steps of:

receiving a secret pattern on a graphical interface, wherein the secret pattern comprises a sequence of discrete graphical choices; converting each discrete graphical choice in the sequence of discrete graphical choices into a value to produce a sequence of values, wherein the sequence of values corresponds to the sequence of discrete graphical choices (column 2, lines 10-45, also figures 4-5, i.e. different graphical choices are made to form codewords);

for a sequence of values, selecting a codeword from a plurality of codewords for each value in the sequence the values, the plurality of codewords being associated with an ... code; for the sequence of values, calculating a security value of a security parameter and the sequence of codewords; and comparing the security value of the security parameter to a threshold value (column 2, lines 10-45, also figures 4-5, i.e. different graphical choices are made to form codewords).

These passages of Cottrell do not teach "error-correcting" in the sense of the claim.

Nevertheless, it was well known in the art to have a "error-correcting" situation in computer entry for the motivation of permitting ease of entry of data (by permitting a reasonable amount of error in entry)

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to modify Cottrell for the motivation noted in the previous paragraphs so as to teach the claimed invention.

Regarding claim 2 (entropy, etc.), such particular features are well known in the art for the motivations of ease of programming and of security.

Regarding claim 3 (minentropy, etc.), such particular features are well known in the art for the motivations of ease of programming and of security. Regarding claims 4-8, such particular features are well known in the art for the motivations of ease of programming and of security.

Regarding claim 9, Cottrell teaches "A method for establishing a secret to authenticate a user comprising the steps of:

receiving a secret pattern on a graphical interface, wherein the secret pattern comprises a sequence of discrete graphical choices; converting each discrete graphical choice in the sequence of discrete graphical choices into a value to produce a sequence of values, wherein the sequence of values corresponds to the sequence of discrete graphical choices' (column 2, lines 10-45, also figures 4-5, i.e. different graphical choices are made to form codewords),

selecting a codeword from a plurality of codewords for each value in the sequence of values to generate a sequence of codewords, the plurality of codewords being associated with an ... code; calculating an offset between each value in the sequence of values and the corresponding codeword in the sequence of codewords to generate a sequence of offsets; and hashing the sequence of codewords to produce a

hash of the sequence of codewords (column 2, lines 10-45, also figures 4-5, i.e. different graphical choices are made to form codewords)."

These passages of Cottrell do not teach "error-correcting" in the sense of the claim.

Nevertheless, it was well known in the art to have a "error-correcting" situation in computer entry for the motivation of permitting ease of entry of data (by permitting a reasonable amount of error in entry)

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to modify Cottrell for the motivation noted in the previous paragraphs so as to teach the claimed invention.

Regarding claim 10 (point in graphical interface, etc.), such particular features are well known in the art for the motivations of ease of use and of security.

Regarding claim 11 (displaying image, etc.), such particular features are well known in the art for the motivations of ease of use and of security. Regarding claims 12-58, such particular features are well known in the art for the motivations of ease of programming and of security.

Regarding claim 59, Cottrell teaches "A method for generating a cryptographic secret from a visual password, the method comprising the steps of:

receiving a secret pattern on a graphical interface, wherein the secret pattern comprises a sequence of discrete graphical choices; converting each discrete graphical choice in the sequence of discrete graphical choices into a value to produce a sequence of values, wherein the sequence of values corresponds to the sequence of discrete

Art Unit: 2134

graphical choices (column 2, lines 10-45, also figures 4-5, i.e. different graphical choices are made to form codewords);

selecting a codeword from a plurality of codewords for each value in the sequence of values to generate a sequence of codewords, the plurality of codewords being associated with an ... code; and manipulating the sequence of codewords to produce a cryptographic secret (column 2, lines 10-45, also figures 4-5, i.e. different graphical choices are made to form codewords).

These passages of Cottrell do not teach "error-correcting" in the sense of the claim.

Nevertheless, it was well known in the art to have a "error-correcting" situation in computer entry for the motivation of permitting ease of entry of data (by permitting a reasonable amount of error in entry)

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to modify Cottrell for the motivation noted in the previous paragraphs so as to teach the claimed invention.

Regarding claim 60 (use of offsets to generate codewords, etc.), such particular features are well known in the art for the motivations of ease of programming and of security.

Regarding claim 61 (use of error-correcting codes to generate codewords, etc.), such particular features are well known in the art for the motivations of ease of programming and of security. Regarding claims 62-71, such particular features are well known in the art for the motivations of ease of programming and of security.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Points of Contact

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, D.C. 20231

or faxed to:

Art Unit: 2134

(703) 746-7239, (for formal communications intended for entry)

Or:

(703) 746-5606 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Jung whose telephone number is (571) 272-3836 or Greg Morse whose telephone number is (571) 272-3838.

David Jung

Patent Examiner

5/16/05

A handwritten signature in black ink, consisting of a large, stylized 'D' followed by a series of loops and a long horizontal stroke.